Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) organised by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

A Study on Manet and Its Security Issues

Mr.S.Prasath
Department of Computer Science,
Assistant professor,
Veltech Ranga Sanku Arts College, Chennai
prasathinba16@gmail.com

Abstract

MANET is defined as mobile ad hoc network; MANET is an infrastructure less wireless connection. The MANETs are mobile, they use wireless connection to connect various network. The Ad-hoc network can change location and configure itself on the fly. In operation, the nodes of a MANET do not have a centralized administration mechanism where each nodes act as a "router" to forward the traffic to other specified node in the network. MANET enabling devices to create and join networks "on the fly"-anywhere anytime. The challenges in MANET are routing, power consumption, autonomous, dynamic topology, limited resource. In this paper we discuss about the MANET architecture, features, and security issues related wireless network.

Keywords: MANET, architecture, features, attack.

1. Introduction

Ad-hoc network are autonomously self-organized networks without any infrastructure support. The ad-hoc network nodes usually have limited transaction range and so some nodes cannot directly communicate with each other. Ad-hoc networks do not depend on any pre-established infrastructure so they can be easily deployed in disaster recovery situations and non-existing or damaged communication infrastructure where speedy employment of a communication network is preferred [9]. Mobile Ad-hoc network is a gathering of remote nodes that can be set up anywhere and anytime without the intervention of existing network. As we definitely know, portable framework is free to move and often act as routers as well as hosts Connected to wireless links [3].

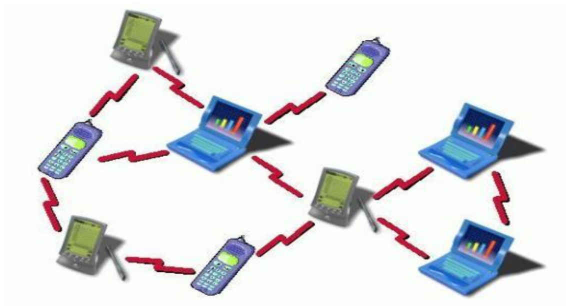

Fig-1.1 MANET

MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANET is more prone to malicious attacks [2]. The main goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes may be combined routers and hosts they form the network routing infrastructure in an ad-hoc fashion. The advantage of MANETs is ease of deployment, speed of deployment and cost of deployment.

2. Features of MANET

Multi-hop Routing: Single hop and multi-hop are the basic types of ad hoc routing algorithms. If we talking about the structure and implementation then single-hop MANET simpler than multi-hop. Delivering packets in multi-hop are transmitted through more than one node to the destination [3].

Partitioned operation: The nodes engaged in a MANET should cooperate among themselves. Every node is behaving like a relay [4].

Autonomous Terminal: Nodes in MANET can serve the function of the host as well as perform functions as router [3].

Fluctuating link capacity: In MANET one communication path is shared by many sessions. The channel on which the nodes communicate is subjected to noise, fading, and interference, and has less bandwidth than a guided network. In some cases the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous [4].

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) organised by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

Light weight terminals: Mostly MANET nodes are mobile devices with less CPU processing capability, small memory size and low power storage [4].

Self-directed terminal: Each mobile node in the ad-hoc networks behaves both host and router. It means that nodes are sending the packet and also forward the packet or route the packet. [3]

Dynamic Network Topology: The Network topology may change rapidly and unpredictably as nodes are mobile. Nodes that lie within each other's range can impart straightforwardly and are in charge of progressively finding each other. [3]

Distributed Operation: It exist no central control system in the background. The control and management operation of networks are distributed among terminals only. All nodes are collaborated and work themselves and each node acts as needed. [3]

3. Architecture of MANET

The MANET is wireless network, it will connect network without any central administration. The basic architecture view of MANET is show below,

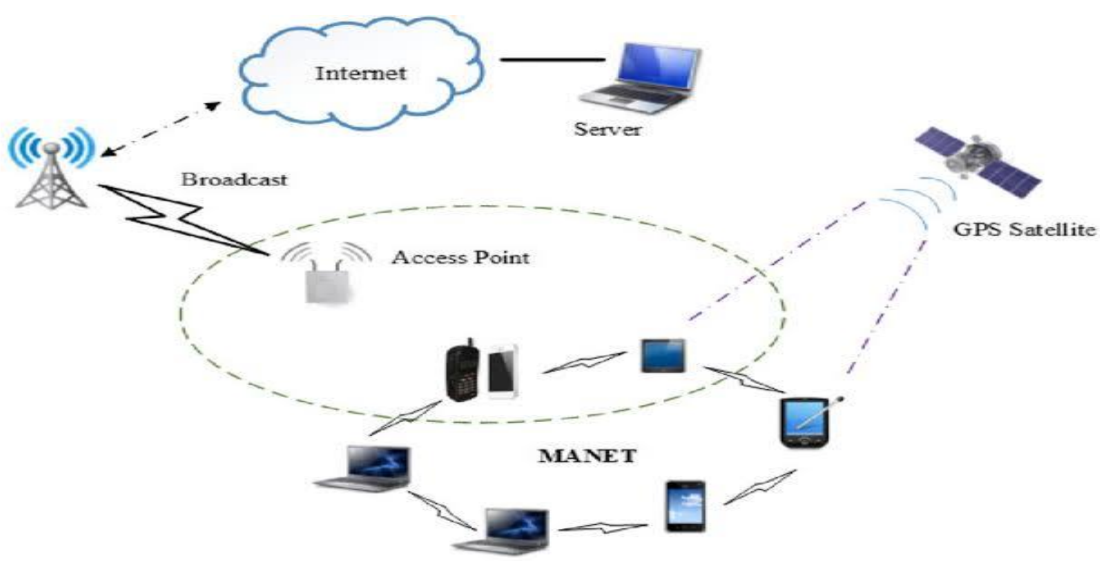

Fig-3.1 Basic architecture view of MANET

The architecture of MANET can be divided into three parts are;

- Enabling technologies
- Networking

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) organised by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

- Middleware and applications

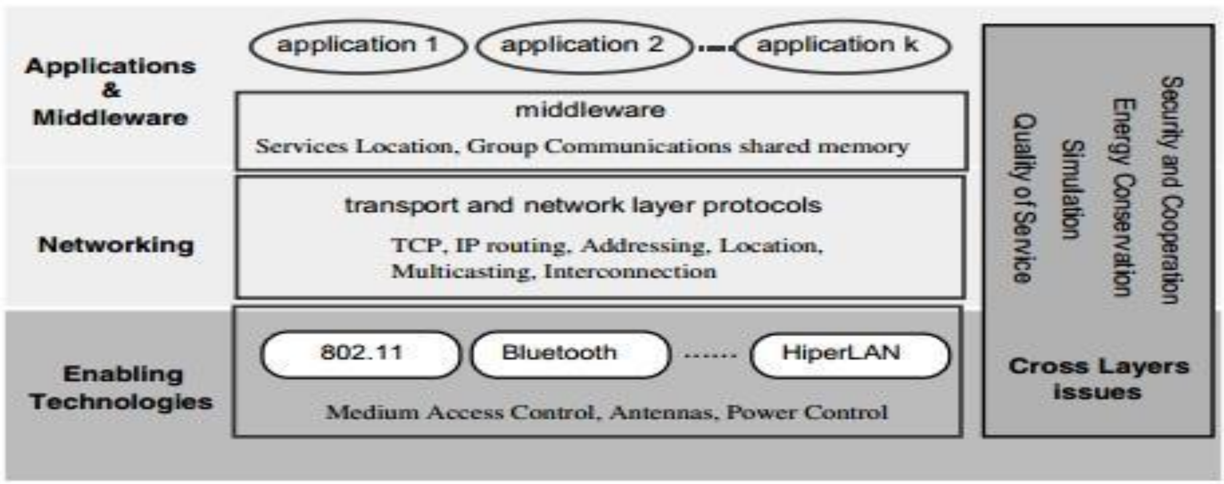

Fig-3.2 Architecture of MANET

Enabling technologies

These are further divided into various classes like,

- BAN (Body Area Network): the BAN provides the connectivity to devices that may be attached to wearable computers. The Communication range is 1-2 meters.
- PAN (Personal Area Network): the PAN connects the mobile devices to another mobile devices or stationary devices. The communication range is 10 meters.
- WLANs (Wireless local area network): the WAN and MAN are mobile multi-hop wireless networks that still facing various challenges like security, addressing etc.

Networking

The initial target of networking protocols is to use the one-hop transmission services, given by the enabling technologies to evolve end-to-end reliable services, from a sender to the receiver [4]. To inculcate an end-to-end communication the sender needs to find the receiver inside the network. The major task of a location service is to dynamically map the address of the receiver device to its present location in the network [4].

Middleware and applications

The wireless technologies like Wi-Fi, Bluetooth, IEEE 802.11, WiMAX and Hyper LAN remarkably encourages the deployment of ad hoc technology and new ad hoc networking applications mainly in specific fields like emergency services, disaster recovery and environment monitoring[4]. The versatility of MANET makes this innovation adaptive for some practical

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) organised by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

situations like, in PAN, home networking, law enforcement operation, commercial and educational applications, and sensor network. Mobile ad hoc frameworks recently created adopt the methodology of not having a middleware, yet rather depend on every application to handle every one of the services it needs[4].

4. Security Issues in MANET

The MANET security issues are respect to data confidentiality, availability of systems and application, and system integrity. The vulnerabilities can lead to message eavesdropping, injection of fake message, denial of service attack (DOS), poor monitoring of routing information, no secure boundaries, lack of centralized management, power and computational limitations and cooperativeness. These can be categorized into two attack are passive attack and active attack. The passive attack will only monitored not inject any fake information. The some of the passive attack are eavesdropping, traffic analysis and snooping. The active attack is an effective violation on either the network resources or the data transmitted. Some of active attack are denial of service, gray hole attack, black hole attack, worm hole attack, packet modification and impersonation.

4.1 Passive attack

The passive attack will only monitored not inject any fake information. The some of the passive attack are eavesdropping, traffic analysis and snooping. This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully [2].

Eavesdropping

The node will simply observe the confidential information during communication. The confidential information may include the location, public key, private key or even passwords of the nodes [7].

Traffic Analysis

In this attack, the attacker scrutinizes the traffic, determine the location, discover communicating hosts, it detects the frequency and length of message being exchanged [7]. Process of collecting information on the way to keep track of essential information in communication, or in other words gathers all the information of the network [6].

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) organised by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

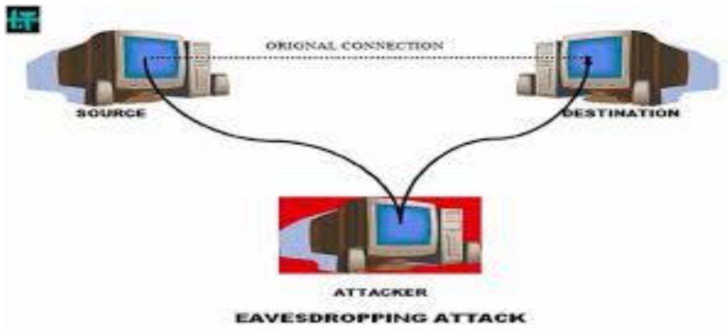

Fig-4.1 Eavesdropping Attack

Snooping

Snooping is unauthorized access to another person's data. It is similar to Eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing [2].

4.2 Active Attack

Active attacks are the attacks that are done by the malicious nodes. These nodes consume some energy in order to perform the attacks. Active attacks involve some changes of data or creation of false information [2]. The active attack is an effective violation on either the network resources or the data transmitted. Some of active attack are denial of service, Gray hole attack, black hole attack, worm hole attack, packet modification and impersonation. this is done by International Journal on New Computer Architectures and Their Applications causing routing disruption, network resource depletion, and node breaking[2].

Denial of Services (DOS)

The DOS makes a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting service of a host connected to the internet. Also, the mobile ad hoc networks are more vulnerable than the wired networks. The interference-prone radio channel and the limited battery power is the reason behind the vulnerability [7].

Gray-Hole Attack

This attack is known as a routing misbehavior attack which leads to packet loss. Gray-hole attack has two phases, the first phase the node advertise itself as having a valid route to destination and second phase, nodes drops intercepted packets with a certain probability [2]. The functionalities of the gray-hole node are each incoming UDP packets are dropped partially with random collection process, that kind of attacker node can change character from genuine to sinkhole, Since it performance as a normal node change over to malicious node it develop also typical to identify the State whether it us original or malicious node [8].

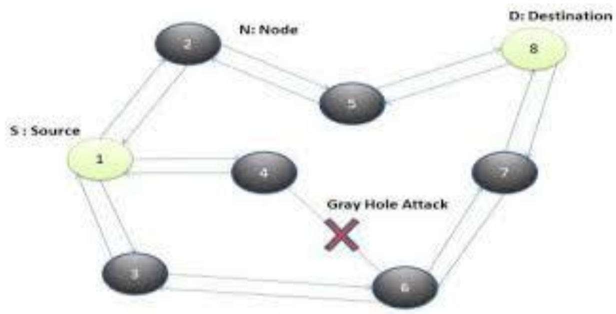

Fig-4.2 Gray-Hole Attack

Black Hole Attack

In Black hole attack the malicious node publicize itself as having best path in route discovery process, As soon as it receives the RREQ packets it will send fake RREP packet to source node [6]. Route discovery process in AODV is vulnerable to the black hole attack. The mechanism is that any intermediate node may respond to the RREQ message if it has a fresh enough routes it devised to reduce routing delay and is used by the malicious node to compromise the system.

In this attack the malicious node listens to a route request packet in the network it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it [2].

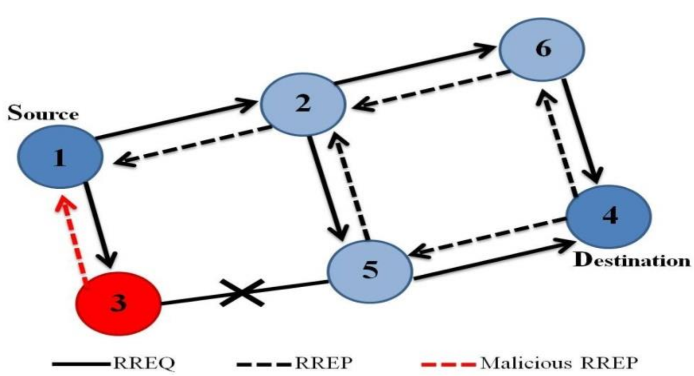

Fig-4.3 Example of black hole attack

Worm Hole Attack

This route between two malicious nodes forms a tunnel called wormhole, this attack the malicious node receives data packet from source node and will forward it to another node in a network making it as a malicious, and these are extreme threats to routing protocols [6]. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network [2]. Wormholes are dangerous because they will damage without knowing the network.

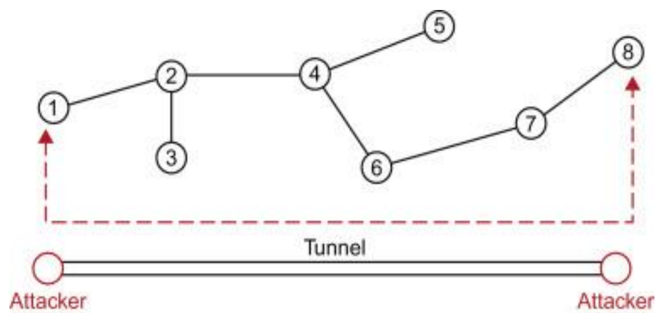

Fig-4.4 Example of Wormhole Attack

Malicious code attacks

Malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application [2].

Jamming

Jamming is a special class of Denial of service attacks which are initiated by malicious node after determining the frequency of communication, this type of attack the jammer transmits signals along with security threats, Jamming attacks also prevents the reception of legitimate packets [2].

Conclusion

The mobile ad hoc network are more vulnerable and have security issues, the nodes of a mobile ad hoc network do not have a centralized administration mechanism, so there is no physical administration it causes more vulnerable, This paper given a general view of a mobile ad hoc network and the attack in the mobile ad hoc network. This paper will helpful to review about the mobile ad hoc network and its security issues to the researcher. The mobile device which forms a self-organizing, self-creating and self-administrating a wireless network is called as a mobile ad hoc network (MANET). Mobile ad hoc network is an infrastructure less wireless connection. The security issues in mobile ad hoc network are managed by some security mechanism. In general the security mechanism of mobile ad hoc network is intrusion detection technique and secure routing technique, this technique the security attack is prevented. This paper will helpful to researcher to understand about the mobile ad hoc network and the security issues.

Reference

[1] A.L.Sandoval Orozco, J.Garcia Matesanz, L.J.Garcia Villalba, J.D. Marques Diaz, and T.H. Kim, "Security Issues in Mobile Ad Hoc Networks".
[2] Mr. L Raja, Capt. Dr. S Santhosh Baboo, "An Overview of MANET:Applications, Attacks and Challenges".
[3] Ishu Varshney, Shahjahan Ali, "STUDY ON MANET: CONCEPTS, FEATURES AND APPLICATIONS".
[4] Sadiya Mirza, Sana Zeba Bakshi, Student M. Tech. 1st Year, Dept. of Electronics & Communication Engineering, "Introduction to MANET"
[5] http://studylap-manet.blogspot.com/2015/09/characteristics-of-manet-m-obile-dhoc.html
[6] Pimal Khanpara, " SECURITY ISSUES IN MANETS".
[7] Sarika Sa, Assistant Professor, Department of Computer Science and Engineering, Sathyabama University,Chennai, India Pravin Ab, Assistant Professor, Department of Computer Science and Engineering, Sathaybama University,Chennai, India, Vijayakumar Ac, Professor, Department of Information Technology, Jerusalem College of Engineering, Anna University, Selvamani Kd, dAssistant Professor, Department of Computer Science and Engineering, Anna University "Security Issues In Mobile Ad Hoc Networks".
[8] M. Jeevamaheswari*, R. Anandha Jothi, V. Palanisamy ,Department of Computer Applications, Alagappa University, Karaikudi, "AODV Routing Protocol to Defence Against Packet Dropping Gray Hole Attack In MANET".